P8, L10

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－106694
(P2000－106694A)
(43)公開日　平成12年４月11日(2000.4.11)

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
Ｈ０４Ｑ	7/38		Ｈ０４Ｂ 7/26	１０９Ｓ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ 1/00	６６０Ｂ	５Ｋ０２５
Ｈ０４Ｌ	9/32		Ｈ０４Ｍ 15/00	Ｇ	５Ｋ０３０
	12/14		Ｈ０４Ｂ 7/26	１０９Ｊ	５Ｋ０６７
Ｈ０４Ｍ	15/00		Ｈ０４Ｌ 9/00	６７５Ｄ	

審査請求　未請求　請求項の数９　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平10－274070

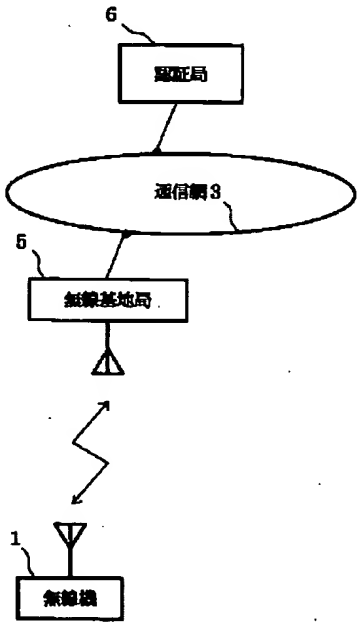
(22)出願日　平成10年９月28日(1998.9.28)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　尾林　秀一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100077849
弁理士　須山　佐一

最終頁に続く

(54)【発明の名称】　無線通信装置および無線通信システム

(57)【要約】
【課題】ＩＣカードなどの電子課金用デバイスを用いて無線通信システムでの無線機による無線通信を行う場合に、より安全な認証を行うとともに認証に関わる使用者の負担を低減する。
【解決手段】この無線通信システムに用いられる無線機１は、電子課金用デバイス１２との信号をやりとりする電子課金用デバイス入出力ポート１３と、電源が入力された状態で電子課金用デバイス入出力ポート１３での信号のやりとりが可能になった事象、あるいは電子課金用デバイス入出力ポート１３に電子課金用デバイス１２が装着された状態で電源が投人された事象を検出し、これらの事象を検出したときのタイミングに応じて異なる手順で認証手順を開始する認証開始制御部１４とを備える。



【特許請求の範囲】

【請求項１】　使用者の認証を行なう認証局を介し、電子的な課金を行なう無線通信システムで使用される無線通信装置において、

入出力される前記電子的な課金に関する電子課金データを記憶保持する電子課金手段と、

この電子課金手段に対し電源を供給する電源供給手段と、

この電源供給手段によって前記電子課金手段に電源が供給されたかどうかを検出する検出手段と、

この検出手段により前記電子課金手段に電源が供給されたことが検出された場合に、前記電子課金データを前記認証局宛に送出する認証制御手段とを具備したことを特徴とする無線通信装置。

【請求項２】　使用者の認証を行なう認証局を介し、電子的な課金を行なう無線通信システムで使用される無線通信装置において、

前記電子的な課金に関する電子課金データを記憶保持する電子課金手段と、

前記電子課金手段との前記電子課金データの入出力を行なう入出力手段と、

前記入出力手段によって前記電子課金データの入出力が可能となったことを検出する検出手段と、

前記検出手段により前記電子課金データの入出力が可能となったことが検出された場合に、前記電子課金データを認証局宛に出力する認証制御手段とを具備したことを特徴とする無線通信装置。

【請求項３】　前記電子課金データは、前記無線通信装置の使用者を特定する情報であることを特徴とする請求項１または請求項２記載の無線通信装置。

【請求項４】　前記電子課金手段は、無線通信装置本体から取り外し可能であることを特徴とする請求項１または請求項２記載の無線通信装量。

【請求項５】　前記電子課金手段およびまたは前記認証制御手段は、無線通信装置本体と着脱ができないよう一体的に構成されたことを特徴とする請求項１または請求項２記載の無線通信装置。

【請求項６】　前記電子課金手段は、無線通信装置本体から取り外し可能であり、かつ前記入出力手段は、単一種類の前記電子課金手段とのみ接続可能な形状からなることを特徴とする請求項２記載の無線通信装量。

【請求項７】　前記電子課金データは、少なくとも無線通信装置の使用者を特定するための暗号鍵と、前記使用者が使用可能な無線通信システムの種別情報とを含んでいることを特徴とする請求項１または請求項２記載の無線通信装置。

【請求項８】　使用者の認証を行なう認証局を介し、電子的な課金を行なう無線通信システムにおいて、

少なくとも無線通信装置の使用者を特定するための暗号鍵と、前記使用者が使用可能な無線通信システムの種別情報とを含む前記電子的な課金に関する電子課金データを記憶保持する電子課金手段と、

前記電子課金手段との前記電子課金データの入出力を行なう入出力手段と、

前記入出力手段を介して前記電子課金データを参照し、該電子課金データに基づき電子的な課金を行なう手段とを具備したことを特徴とする無線通信システム。

【請求項９】　複数の無線通信システムにそれぞれ対応した複数の通信用ソフトウェアを記憶する記憶手段と、

前記複数の通信用ソフトウェアのうち一つを利用して前記基地局と無線通信を行なう無線通信手段と、

前記無線通信手段が無線通信を行なっている前記基地局から、前記複数の通信用ソフトウェアのうち一つの使用を許可する暗号鍵を受信する受信手段と、

この受信手段により受信された前記暗号鍵に基づいて、前記記憶手段に記憶されている複数の通信用ソフトウェアから少なくとも一つの通信用ソフトウェアを選択して前記無線通信手段に設定する手段とを具備したことを特徴とする請求項１または請求項２記載の無線通信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば無線通信装置および無線通信システムに関する。

【０００２】

【従来の技術】現在、携帯電話をはじめとする無線通信システムは、システムを利用する携帯電話の利用者に対して課金を行っているが、この場合、予め事業者と加入者間での契約条件・通話相手・通話時間などの課金に関する情報が基地局・制御局側に記録され、１ヶ月などの期間内の記録に基づきシステムの利用料金が計算され、加入者に請求するという方法がとられている。この課金形態では、課金処理をオフラインで行うしかない。

【０００３】一方、公衆自動車電話などの不特定多数の使用者が用いる用途で列車、バス、飛行機などの移動体に設置される無線通信機では、課金処理はプリペイドカードや硬貨などでオンラインで行われることもある。

【０００４】しかし、無線通信システム事業者が無線通信機を設置される移動体と関連付けて信頼できるものと仮定し、その移動体の認証を行っているにすぎない。また、課金に関するチェックは、一般の公衆電話と同様にプリペイドカードや硬貨などが不正なものでないことを確認しているにすぎない。また、クレジットカードによる通話に関しても、一定のマニュアルに従ってオペレータが本人の電話番号などを確認するようなマニュアル的な認証を行っていたり、数けた程度の暗証番号を携帯端末から入力するといったやり方が行われている。

【０００５】一方、近年、ＩＣカードなどの電子課金デバイスを使った電子決済の実験などが行われているが、これを一般の携帯電話に応用することを仮定した場合、上記した従来の課金形態では、せいぜいマニュアル的な

認証や暗証番号などによる認証にとどまり、電話機の改造・偽造や加入者になりすますなどの悪意の利用者による不正行為などに対するセキュリティの確保が十分ではないという現実がある。

【０００６】

【発明が解決しようとする課題】このように上述した従来の無線通信システムでは、ＩＣカードなどの電子課金デバイスを用いて電子的な課金を行う上では、せいぜいマニュアル的な認証や暗証番号などによる認証にとどまり、携帯電話、つまり無線通信装置の改造・偽造や加入者になりすますなどの悪意の利用者による不正行為に対するセキュリティが十分でないという問題があった。

【０００７】本発明はこのような課題を解決するためになされたもので、電子課金デバイスを用いて電子課金を行う上で、より安全に認証を行うと共に、認証に関わる使用者の負担を軽減でき、さらに課金のための記録容量を削減することができる無線通信装置および無線通信システムを提供することを目的としている。

【０００８】

【課題を解決するための手段】上記した目的を達成するために、請求項１記載の発明の無線通信装置は、使用者の認証を行なう認証局を介し、電子的な課金を行なう無線通信システムで使用される無線通信装置において、入出力される前記電子的な課金に関する電子課金データを記憶保持する電子課金手段と、この電子課金手段に対し電源を供給する電源供給手段と、この電源供給手段によって前記電子課金手段に電源が供給されたかどうかを検出する検出手段と、この検出手段により前記電子課金手段に電源が供給されたことが検出された場合に、前記電子課金データを前記認証局宛に送出する認証制御手段とを具備したことを特徴としている。

【０００９】この請求項１記載の発明では、電源供給手段が電源の供給を開始したことを検出すると、認証を開始するので、認証に関わる作業を使用者本人が行う必要がなくなり、使用者の作業負担を軽減することができる。

【００１０】請求項２記載の発明の無線通信装置は、使用者の認証を行なう認証局を介し、電子的な課金を行なう無線通信システムで使用される無線通信装置において、前記電子的な課金に関する電子課金データを記憶保持する電子課金手段と、前記電子課金手段との前記電子課金データの入出力を行なう入出力手段と、前記入出力手段によって前記電子課金データの入出力が可能となったことを検出する検出手段と、前記検出手段により前記電子課金データの入出力が可能となったことが検出された場合に、前記電子課金データを認証局宛に出力する認証制御手段とを具備したことを特徴としている。

【００１１】請求項２記載の発明では、カードが使用できるかどうかを検出すると、認証を開始するので、終了した後の待受け状態下で、少なくとも１つの無線通信システムを使用するための要求があると、この要求に応じた通信用のソフトウェアのディジタル記録素子へのロードを開始するので、ソフトウェアのロードを使用者本人が行う必要がなくなり、使用者の作業負担を軽減することができる。

【００１２】請求項３記載の無線通信装置は、請求項１または請求項２記載の無線通信装置において、前記電子課金データは、前記無線通信装置の使用者を特定する情報であることを特徴としている。

【００１３】請求項３記載の発明では、電子課金データを無線通信装置の使用者を特定する情報としたことで、使用者によるデータ入力操作の負担をなくすことができる。請求項４記載の無線通信装置は、請求項１または請求項２記載の無線通信装置において、前記電子課金手段は、無線通信装置本体から取り外し可能であることを特徴としている。

【００１４】この請求項４記載の発明では、電子課金手段を、無線通信装置本体から取り外し可能にしたことで、通信時以外は電子課金手段を無線通信装置本体から取り外しておけば、無線通信装置本体が盗難あるいは紛失した場合でも、それを取得した悪意の利用者によって無線通信装置無断が利用されることがなくなる。

【００１５】請求項５記載の発明の無線通信装置は、請求項１または請求項２記載の無線通信装置において、前記電子課金手段およびまたは前記認証制御手段は、無線通信装置本体と着脱ができないよう一体的に構成されたことを特徴としている。

【００１６】請求項５記載の発明では電子課金手段および、または認証制御手段を無線通信装置本体から取り外し不可能に一体的に構成したことで、無線通信装置が悪意の利用者に渡った場合にそれが改造されたり偽造されることを防止でき、例えば悪意の利用者が加入者本人になりすまし課金を逃れるような不正行為を行うことを防止できる。

【００１７】請求項６記載の発明の無線通信装置は、請求項２記載の無線通信装置において、前記電子課金手段は、無線通信装置本体から取り外し可能であり、かつ前記入出力手段は、単一種類の前記電子課金手段とのみ接続可能な形状からなることを特徴としている。

【００１８】この請求項６記載の発明では、電子課金手段を、無線通信装置本体から取り外し可能であり、かつ電子課金手段の入出力手段を単一種類の電子課金手段とのみ接続可能な形状としたことで、電子課金手段と無線通信装置本体との組み合わせを変えることを不可能にし、いずれか一方を取得した悪意の利用者による無線通信システムの利用を防止することができる。

【００１９】請求項７記載の発明の無線通信装置は、前記電子課金データは、少なくとも無線通信装置の使用者を特定するための暗号鍵と、前記使用者が使用可能な無線通信システムの種別情報とを含んでいることを特徴と

している。

【００２０】この請求項７記載の発明では、電子課金データに、このデバイスを使用する使用者を特定するための暗号鍵と、使用者が使用可能な無線通信システムの種別情報とを含ませたことで、電子課金デバイスにて使用者本人が行わずとも、自動的に本人認証を行ったり、所望の無線通信システムの通信用ソフトウェアのロードを行うことができる。また、この電子課金データを用いることによって、無線機使用者に関する認証手順のうちの、本人認証以外のかなりの部分を削減し、速やかな認証作業を行えると共に基地局・制御局側の制御を低減することができる。さらに暗号鍵や無線通信システムの種別情報を電子課金データとして電子課金手段に記録しておくことで、予め認証手続きやソフトウェアのロードに必要な情報の記録が最低限で済み、課金のための記録容量を削減することができる。

【００２１】請求項８記載の発明の無線通信システムは、使用者の認証を行なう認証局を介し、電子的な課金を行なう無線通信システムにおいて、少なくとも無線通信装置の使用者を特定するための暗号鍵と、前記使用者が使用可能な無線通信システムの種別情報とを含む前記電子的な課金に関する電子課金データを記憶保持する電子課金手段と、前記電子課金手段との前記電子課金データの入出力を行なう入出力手段と、前記入出力手段を介して前記電子課金データを参照し、該電子課金データに基づき電子的な課金を行なう手段とを具備したことを特徴している。

【００２２】この請求項８記載の発明では、少なくとも無線通信装置の使用者を特定するための暗号鍵と、使用者が使用可能な無線通信システムの種別情報とを含む電子的な課金に関する電子課金データを記憶保持した電子課金手段を無線通信装置に装着し、無線通信装置が所望の無線通信システムと通信を行う際に、電子課金手段の暗号鍵と種類情報を含む電子課金データを参照して電子的な課金を行うので、認証を安全に行うと共に、課金処理をリアルタイムに行うことができる。

【００２３】請求項９記載の発明の無線通信装置は、複数の無線通信システムにそれぞれ対応した複数の通信用ソフトウェアを記憶する記憶手段と、前記複数の通信用ソフトウェアのうち一つを利用して前記基地局と無線通信を行なう無線通信手段と、前記無線通信手段が無線通信を行なっている前記基地局から、前記複数の通信用ソフトウェアのうち一つの使用を許可する暗号鍵を受信する受信手段と、この受信手段により受信された前記暗号鍵に基づいて、前記記憶手段に記憶されている複数の通信用ソフトウェアから少なくとも一つの通信用ソフトウェアを選択して前記無線通信手段に設定する手段とを具備したことを特徴としている。

【００２４】請求項９記載の発明では、受信手段により受信された暗号鍵に基づいて、記憶手段に記憶されている複数の通信用ソフトウェアから少なくとも一つの通信用ソフトウェアを選択して無線通信手段に設定するので、複数の通信システムに対応し、相手の要望によって、利用するシステムを切り替えることができる。

【００２５】このように本発明によれば、例えば電子課金デバイスなどの電子課金手段を用いた無線通信を行う上で、より安全な認証を行うと共に、認証に関わる使用者の負担を軽減でき、さらに課金のための記録容量を削減することができる。

【００２６】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して詳細に説明する。

【００２７】図１は本発明に係る無線通信装置、電子課金デバイスおよびこれらを用いた無線通信システムの一つの実施の形態である無線通信システムの構成を示す図、図２はこの無線通信システムに用いる無線機の構成を示す図である。

【００２８】近年、セルラー電話システム（Personal digital Cellular System：ＰＤＣ）や簡易型コードレス電話システム（Personal Handyphone System：ＰＨＳ）などの無線通信システムはシステム規模を拡大する中で、事業としての統合化も行われつつあり、このような流れに無線通信装置の機能や課金形態を対応させる必要がある。

【００２９】本発明の一つの実施の形態である無線通信システムは、図１に示すように、インターネットなどの通信網３に無線基地局５および認証局６を接続する一方、無線基地局５は自身のサービスエリア内に存在する無線通信装置１（以下無線機１と呼ぶ）と無線通信するよう構成されている。

【００３０】図２に示すように、無線機１は、利用者によりＯＮ・ＯＦＦされる電源スイッチ１０と、この電源スイッチ１０がＯＮされて各部に電源供給を開始する電源部１１と、契約者本人以外の人が使用不可能なように電子課金デバイス１２が装着されて、この電子課金デバイス１２との信号をやりとりする電子課金デバイス入出力ポート１３と、電源スイッチ１４が入力された状態で電子課金デバイス入出力ポート１３での信号のやりとりが可能になった事象、あるいは電子課金デバイス入出力ポート１３に電子課金デバイス１２が装着された状態で電源が投入された事象を検出し、各事象を検出した後、自動的に無線基地局５を通じた認証局６との信号の送受を含めた無線通信システムを用いた通信の可否を決定するための電子課金デバイス１２を用いる無線機使用者に関する認証手順を開始する認証開始制御装置１４と、この認証開始制御装置１４により認証後に課金処理を行う課金制御部１５と、アンテナ１６ａを介して無線基地局５と通信する無線通信部１６と、通信用ソフトウェアを記録および読み出し可能な情報記録媒体、例えばＩＣカード１７などを装着する媒体装着および読込部としての

ＩＣカードスロット１８と、無線通信部１６により受信されたソフトウェアをＩＣカードスロット１８を通じてＩＣカード１７にロードする送受信ソフトウェアロード部１９と、無線通信部１６へ無線通信する音声信号やデータなどを入出力するマイク、スピーカなどの入出力デバイス２０と、これら各部を制御するマイクロ・プロセッサ・ユニット（以下ＭＰＵと称す）２１と、送受信ソフトウェアロード部１９によりダウンロードされたソフトウェアが記録される例えばＥＥＰＲＯＭなどからなるメモリ２２とを備えている。なお契約者本人以外の人が使用不可能な電子課金デバイス１２と電子課金デバイス入出力ポート１３との実装構造については後述する。

【００３１】情報記録媒体としては、無線機１が例えばハンディタイプ（携帯型）の場合はＩＣカードなどのカード型メディアを利用するが、この他、例えば車載用などの場合は、大容量記録メディア、例えば光磁気ディスク（ＭＯ）やＤＶＤ－ＲＡＭなどでも良い。

【００３２】電子課金デバイス１２には、所定のアドレス領域に、無線機１の使用者の公開鍵１２１や契約している無線通信システムの種類情報１２２などが書き込まれているメモリ１２３と、入出力インターフェース（以下入出力Ｉ／Ｆと称す）１２４と、これらを制御するＭＰＵ１２５とが設けられている。無線通信システムの種類情報１２２としては、例えばセルラーシステムかＰＨＳかなどの他、異なるサービスを提供するための情報（土曜、日曜は割引が使えないサービス、課金形態が異なるサービス、データ通信サービス、高速通信サービスなどという情報の場合もある）の場合もある。

【００３３】認証局６は、無線基地局５あるいは制御局（図示せず）の指示により、無線機１の使用者が本人であることを証明する認証情報あるいはそれに相当する信号を発行し、これを無線基地局５に送付する。

【００３４】例えば公開鍵方式を用いている場合には、認証局６は、無線機１から基地局５を通じて通知された公開鍵１２１に対して、公開鍵１２１が使用者自身のものであるかどうかを判定し、この判定結果で公開鍵１２１が使用者のものであることが証明されれば、認証情報あるいはそれに相当する信号を発行し、これを無線基地局５に送付する。これにより、無線基地局５がインターネットなどのオープンなネットワークに接続しているような環境でも、課金に必要な認証情報を安全に通信することができる。

【００３５】なお、電子課金デバイス１２との信号をやりとりする電子課金デバイス入出力ポート１３は、接触端子付きのＩＣカードなどの場合は、スロットやソケットや端子など、非接触のＩＣカードなどの場合は無線信号用アンテナやプローブなどになる。

【００３６】ところで、Mitola, J.,"The software radio architecture,"IEEE Communication Magazine, Vol.33, No.5(1995年05月）などで提案されているように、ソフトウェアを変更することにより、異なる無線通信方式の送受信が可能になるような無線機（以下ソフト無線機と称す）が研究開発されている。

【００３７】図３にソフト無線機の構成の一例を示す。同図に示すように、このソフト無線機は、高周波アナログ部２０１、アナログーデジタル変換器（以下ＡＤＣと呼ぶ）２０２、デジタルーアナログ変換器（以下ＤＡＣと呼ぶ）２０３、ディジタル信号の形になったＲＦ信号あるいはＩＦ信号に対して周波数変換やフィルタリングなどと等価な処理を行うディジタルダウンコンバートソフトウェアをロードしたフィールドプログラマブルゲートアレー（以下ＦＰＧＡと呼ぶ）２０４、マルチアクセス方式に対応するモデムのソフトウェアやチャネルコーデックのソフトウェアや音声コーデックのソフトウェアなどをロードしたディジタル信号処理ＩＣ（以下ＤＳＰと呼ぶ）２０５、無線送受信のための制御ソフトウェアをロードする制御ＭＰＵ（以下ＭＰＵとも呼ぶ）２０６、およびＡＤＣ２０２、ＤＡＣ２０３、ＦＰＧＡ２０４、ＤＳＰ２０５、制御ＭＰＵ２０６の動作をつかさどる各クロック源２０７、２０８、２０９、２１０、２１１などから構成されている。

【００３８】このソフト無線機の大きな特徴の一つは、ＦＰＧＡ２０４、ＤＳＰ２０５およびＭＰＵ２０６などのソフトウェアを変更することにより、異なる無線通信システムに対応できることである。

【００３９】高周波アナログ部２０１にはアンテナを介して無線通信信号が入出力され、必要に応じて、帯域制限や周波数変換、信号レベルの増幅・減衰などが行われる。ＡＤＣ２０２は、高周波アナログ部２０１からの信号をディジタルに変換する。通常、高周波アナログ部２０１からの信号そのものをサンプリングする際には、ＡＤＣ２０２は、該信号の搬送波周波数の２倍より大きいサンプリング速度で動作させる。また、高周波アナログ部２０１からの信号の包絡線の振幅や位相から情報を取り出すダウンサンプリング法を採用する場合は、ＡＤＣ２０２の動作速度は、包絡線の周波数スペクトルの主要部の最大周波数の２倍より大きいサンプリング速度になる。ＤＡＣ２０３は、ＤＳＰ２０５からの信号をアナログに変換する。このＤＡＣ２０３は、高周波アナログ部２０１に情報の載ったベースバンド信号あるいは中間周波数信号を搬送波周波数で変調した信号を直接送る場合、搬送波周波数の２倍より大きいサンプリング速度で動作させられる。また、高周波アナログ部２０１に情報の載ったベースバンド信号あるいは中間周波数信号の振幅や位相などを送る場合は、ＤＡＣ２０３の動作速度は、ベースバンド信号あるいは該中間周波数信号の周波数スペクトルの主要部の最大周波数の２倍より大きい速度になる。

【００４０】ＦＰＧＡ２０４とＤＳＰ２０５とＭＰＵ２０６では、ＡＤＣ２０２からの入力を用いて、受信すべ

き情報信号を再現するとともに、送信すべき信号を生成し、ＤＡＣ２０３へ出力する。

【００４１】このようなソフト無線機は、複数の無線通信システムに適用することができる。この場合、図２のような機器構成によってソフトウェアをダウンロードする必要がある。

【００４２】ソフト無線機にソフトウェアをダウンロードするにあたり、事業として有償で行う場合と、無償で行う場合とがある。

【００４３】ここで、無線機１の構成でソフトウェアをダウンロードする場合について説明する。

【００４４】例えばソフトウェアのダウンロードを無償で行う場合、ソフト無線機の電源スイッチをＯＮした後の待受け状態下で、発信者である利用者から特定の１つ乃至複数の無線通信システムを使用するための要求操作が行われ、この要求を送受信ソフトウェアロード部１９が検出すると、送受信ソフトウェアロード部１９はその１つ乃至複数の無線通信システムで送受信するためのソフトウェアのロードを開始する。

【００４５】また、ソフトウェアのダウンロードを有償で行う場合、無線機１では、ソフトウェアのロードを行う前に、まず、電子課金デバイス１２を使った電子決済を行い、ソフトウェアのロードのための料金を即時に支払うことが考えられる。

【００４６】ソフトウェアの発行元から電子決済を行う場合は、無線機１からの無線通信で無線基地局５と呼を接続し、通信網上の、ソフトウェアを発行する業者のサイト（サーバ）と通信を行う。

【００４７】業者のサイト（サーバ）は、電子課金デバイス１２と認証局６とを使った認証手続きを行った後、上記業者のサイトから必要なソフトウェアのみをダウンロードできるキーコードを暗号化して無線機１へ送信する。

【００４８】一方、ＩＣカード１７や光ディスクなどのパッシブメディアから無線通信装置へソフトウェアをダウンロードする場合は、これらの発行元あるいは発行元の権限を代行する業者との電子決済を行うため、上記と同様な無線機１からの無線通信により発行元あるいは代行業者と通信を行う。これにより、ＩＣカード１７の発行元の事業者は、電子課金デバイス１２と認証局６とを使った認証手続きおよび電子決済を行った後、ＩＣカード１７から必要なソフトウェアのみをダウンロードできるキーコードを暗号化して無線機１に送信する。なお、上記認証手続きは、事業者毎に独自の手続きの手順があり、同じ場合も異なる場合もある。

【００４９】無線機１では、無線基地局５からの暗号化されたキーコードが無線通信部１６によって受信されると、無線通信部１６はそのキーコードを復号して送受信ソフトウェアロード部１９を通じてＩＣカードスロット１８に装着されたＩＣカード１７へ送る。またこれと同時に無線通信部１６はキーコードをＭＰＵ２１を経由して課金制御回路１５へ送る。

【００５０】課金制御回路１５は、入力されたキーコードが正しいものであるか否かを判定し、キーコードが正しい場合、要求されたソフトウェアのみをＩＣカード１７内部のソフトウェア保存領域（ＥＥＰＲＯＭなどの所定アドレス領域）からＩＣカードスロット１８を通じてＭＰＵ２１へロードさせ、それがメモリ２２に記録される。

【００５１】なお、前記の第１の事象と第２の事象を検出した場合に、異なる手順で認証を依頼する手続きを開始することも考えられる。

【００５２】例えば、第１の事象が生じる場合は、前記無線通信端末には既に電源が投入されており、第１の事象をはじめその他の事象が起こった場合に生じる割り込みを受け入れる状態となっている。したがって、第１の事象が生じると、前記無線通信靖末のＭＰＵ２１は割り込み処理のルーチンに処理が移ることになる。

【００５３】よって、認証を依頼する手続きをこの割り込み処理のルーチンの一部としておけばよい。

【００５４】一方、第２の事象を生じる場合は、その直前には一部の回路を除き前記無線通信端末には電源が投入されていない場合が多い。したがって、電源投入後、ＭＰＵ２１の初期化から始まり、主要な回路の立上げなどの通信を行う状況を整えるソフトウェアが実行された後に、上記電子課金デバイス１２と上記電子課金デバイス入出力ポートとの信号のやり取りが可能な状態の下であるかどうかを判断するソフトウェアを実行するようにしておくことで、第２の事象の有無を判断する。そして、第２の事象を検出した場合のみ認証を依頼する手続きへ処理が移るようにすることにより、認証開始制御部１４の機能が実現できることになる。

【００５５】なお、上記電子課金デバイス１２と上記電子課金デバイス入出力ポート１３との信号のやり取りが可能な状態の下であるかどうかを判断する方法としては、次に列挙する方法なとが考えられる。

【００５６】まず、上記電子課金デバイス入出力ポート１３に上記電子課金デバイス１２を装着したときに機械的にスイッチが切り替わるような機構を上記電子課金デバイス入出力ポート１３に設けることが考えられる。また、上記電子課金デバイス１２を装着したときに、上記無線通信装置から上記電子課金デバイス入出力ポート１３を通じて上記電子課金デバイス１２に対して信号をやり取りし、上記電子課金デバイス１２が正常に動作しているのを確認した場合に、ＭＰＵ２１からアクセスできるメモリ領域の状態フラグの１つを立てることにより、ＭＰＵ２１などが状況を判断できる。特に、非接触形の電子課金デバイスにはこの方法が適していると考えられる。

【００５７】なお、上記した電子課金デバイス１２のメ

モリ１２２に、公開鍵１２１や電子課金デバイス１２を使用する使用者が契約している少なくとも１つの無線通信システムの種類情報１２２などの他に、さらに使用者の本人認証を行うための暗号鍵を記録しておくことにより、上記実施形態における無線基地局５を通じた認証局６との信号の送受を含めた無線通信システムを用いた通信の可否を決定するための電子課金デバイス１２を用いる無線機使用者に関する認証手順のうちの、本人認証以外のかなりの部分を削減し、速やかな認証作業と基地局・制御局側の制御を低減する効果がある。

【００５８】また、さらにメモリ１２２に課金条件などの契約内容が記録しておくことにより、通信中に使用した無線システム、通信時間、通信の種類、帯域幅、契約条件等に基づき、無線機１を使用する際に、即時的（リアルタイム）に使用金額を引き去るようにもできる。

【００５９】なお、特に無線機１をレンタル商品として用いる場合は、レンタル中に悪意の者による無線機１の改造・偽造などが行われ、上記の認証手続きが不正に行われる可能性は否定できない。

【００６０】そこで、これを防ぐために、図４に示すように、無線機本体４１に取り付ける回路基板４２に、認証開始制御部１４を内蔵したＩＣ４３あるいは電子課金デバイスチップ４４を、例えばエポキシ樹脂などによる熱硬化処理などによって封止し、回路基板４２からの取り外しがほぼ不可能に密封して実装することにより、上記認証制御に重要な役割を果たす認証開始制御部１４や電子課金デバイス１２が着脱できないような構造とする。

【００６１】あるいは、レンタル契約の際に使用料金の上限に相当する料金を上記電子課金デバイス１２にセットしておき、図５に示すように、無線機本体をカード型の筐体（カード型無線機本体５１）として、印刷配線を施した回路基板５２の表面に、ＭＰＵ２１や認証開始制御部１４を内蔵したＩＣ４３あるいは電子課金デバイスチップ４４などを実装後、回路基板５２の実装面全体に樹脂カバー５３などを接着剤などで貼り合わせて一体化し、この一体化したものをカード型無線機本体５１に装着することにより、例えばノート型パーソナルコンピュータのＰＣＭＣＩＡスロットなどに装着するカード型の無線機にでき、しかも、電子課金デバイス１２や認証開始制御部１４をこの無線機をレンタル契約した使用者が取り外そうとして、表面カバー５３を回路基板５２から無理に剥がそうとすると、ＩＣチップや印刷配線が破壊されてしまうので、取り外した電子課金デバイスチップ４４や認証開始制御部１４を内蔵したＩＣ４３などを再使用できない構造とすることができる。

【００６２】また、次善の策ではあるが、図６に示すように、一端部に切り欠き部６１ａ～６１ｃなどと表面に接続用端子（電気接点）６２とをカード型の特定（単一）の電子課金デバイス６３に形成しておき、この特定の電子課金デバイス６３のみに嵌合する突起部６４ａ～６４ｃと接続用端子６２に対応する接続用端子（電気接点）６５とを無線機１の電子課金デバイス入出力ポート１３に設け、電子課金デバイス６３を電子課金デバイス入出力ポート１３に装着して無線機１を使用することにより、ある特定の使用者以外の使用者による電子課金デバイス１２の不正使用行為を抑制することができる。

【００６３】つまり、電子課金デバイス入出力ポート１３の形状を、ある特定の使用者、またはある特定の使用者群が所有する電子課金デバイス６３のみに嵌合する形状にしておき、それ以外の形状をもつ電子課金デバイス１２の使用者による不正行為を抑制する。

【００６４】このようにこの実施の形態の無線通信システムによれば、無線機１内部に電子課金デバイス１２を備え、無線通信による認証処理後に所望の無線通信システムのソフトウェアのダウンロードを行う場合に、電源が入力された状態で電子課金デバイス入出力ポート１３での信号のやりとりが可能になった事象あるいは電子課金デバイス入出力ポート１３に電子課金デバイス１２が装着された状態で電源が投入された事象をそれぞれ検出し、これらの事象が検出されたタイミングに応じて、無線通信システムの無線基地局を通じた認証局６との信号の送受を含めた電子課金用デバイス１２を用いる無線機使用者に関する認証手順を開始するので、より安全な認証を行うと共に認証に関わる使用者の負担を低減することができる。また課金のための情報の記録容量を削減することができる。

【００６５】また、ＭＰＵ２１、認証開始制御部１４、電子課金用デバイスチップ４４などを、無線機から着脱不可能に実装することにより、悪意の使用者による不正行為を防止することができる。

【００６６】さらに、無線機１内の電子課金用デバイス入出力ポート１３の形状を、ある特定の使用者、またはある特定の使用者群が所有する電子課金用デバイス６３に嵌合させる形状とすることにより、上記以外の使用者がもつ電子課金用デバイス１２による不正行為を抑制することができる。

【００６７】

【発明の効果】以上説明したように本発明によれば、電源供給手段が電源の供給を開始したことを検出して認証を開始するので、認証に関わる作業を使用者本人が行う必要がなくなり、使用者の作業負担を軽減することができる。

【００６８】また、電子課金手段および、または認証制御手段を無線通信装置本体から取り外し不可能に一体的に構成したことで、無線通信装置が悪意の利用者に渡った場合にそれが改造されたり偽造されることを防止でき、例えば悪意の利用者が加入者本人になりすまし課金を逃れるような不正行為を行うことを防止できる。

【００６９】さらに、電子課金手段を無線通信装置本体

から取り外し可能に、かつ電子課金手段の入出力手段を単一種類の電子課金手段とのみ接続可能な形状としたことで、電子課金手段と無線通信装置本体との組み合わせを変えることを不可能にし、いずれか一方を取得した悪意の利用者による無線通信システムの利用を防止することができる。

【００７０】また、暗号鍵や無線通信システムの種別情報を電子課金手段に記録しておくことで、予め認証手続きやソフトウェアのロードに必要な情報の記録が最低限で済み、課金のための記録容量を削減することができる。

【００７１】この結果、電子課金用デバイスを用いた一般の携帯電話、つまり無線通信装置による無線通信を行う上で、より安全な認証を行うと共に、認証に関わる使用者の負担を軽減でき、さらに課金のための記録容量を削減することができる。

【図面の簡単な説明】

【図１】本発明の一つの実施の形態の無線通信システムの構成を示す図。

【図２】この無線通信システムに用いられる無線機の構成を示す図。

【図３】ソフト無線機の構成の一例を示す図。

【図４】無線機に認証開始制御部あるいは電子課金デバイスを実装した様子を示す図。

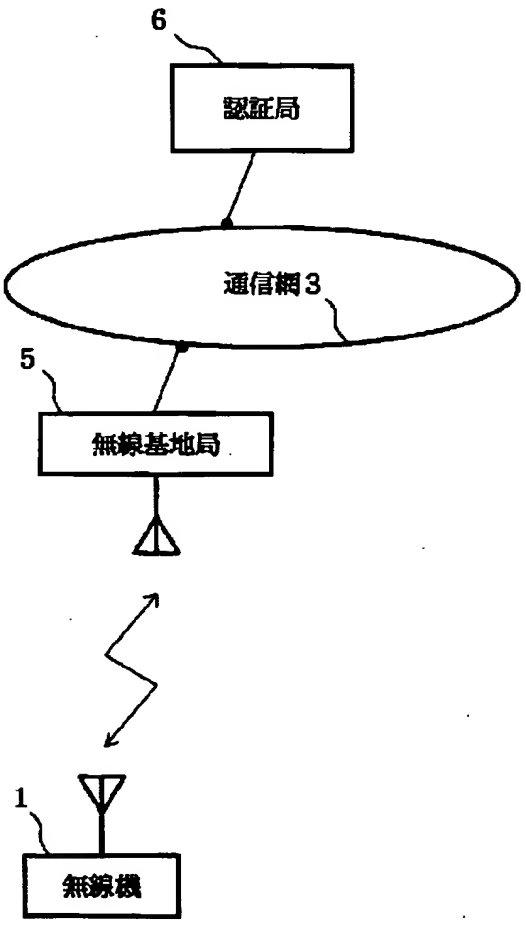
【図５】無線機内に取り付ける基板に認証開始制御部を内蔵したチップあるいは電子課金デバイスチップを実装する様子を示す図。

【図６】無線機本体に挿脱自在な電子課金デバイスの一例を示す図。

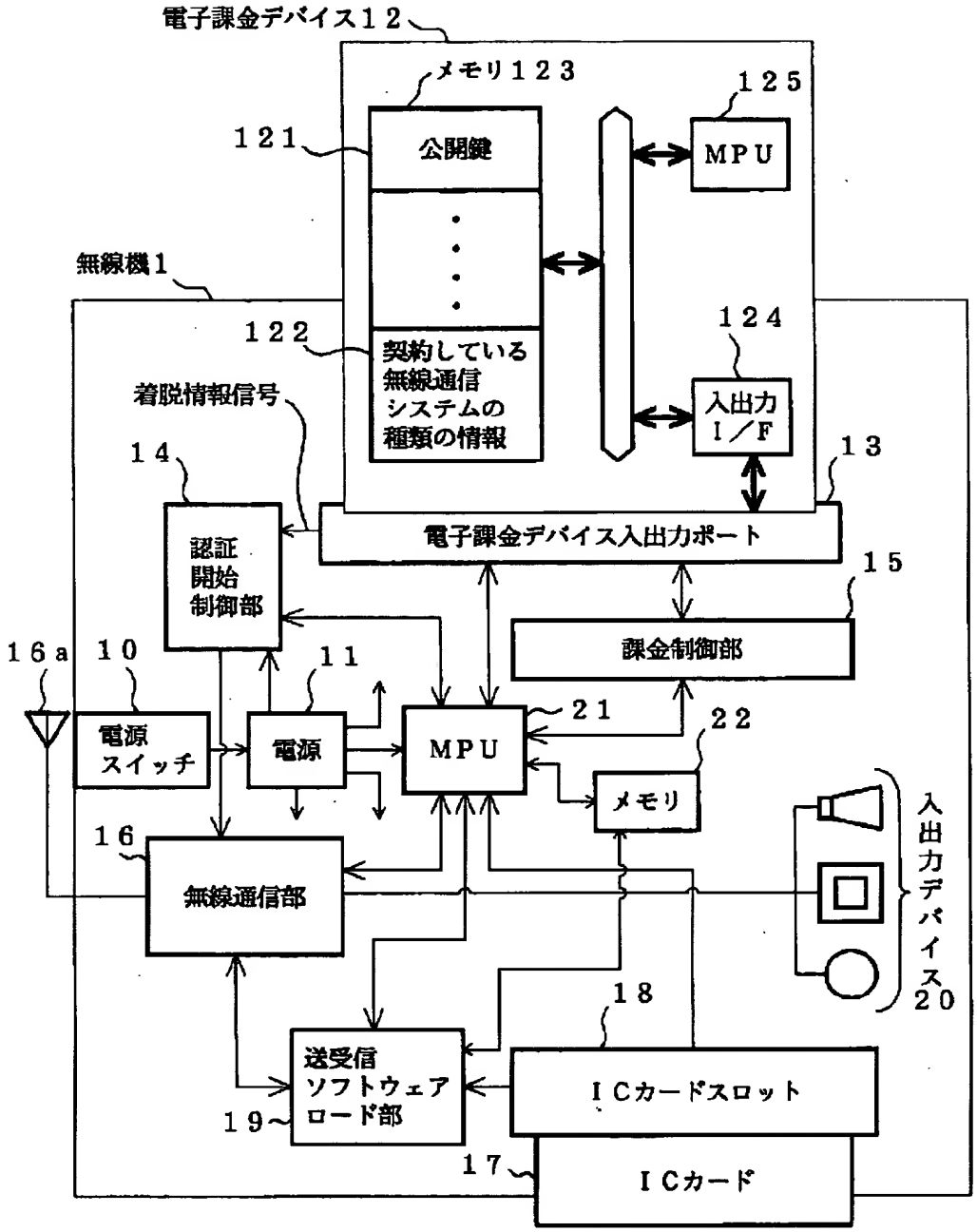
【符号の説明】

１…無線機、３…通信網、５…無線基地局、６…認証局、１０…電源スイッチ、１１…電源、１２…電子課金用デバイス、１３…電子課金用デバイス入出力ポート、１４…認証開始制御部、１５…課金制御部、１６…無線通信部、１７…ＩＣカード、１８…ＩＣカードスロット、１９…送受信ソフトウェアロード部、２０…入出力デバイス、２１…ＭＰＵ、１２３，２２…メモリ、１２４…入出力Ｉ／Ｆ、１２５…ＭＰＵ。

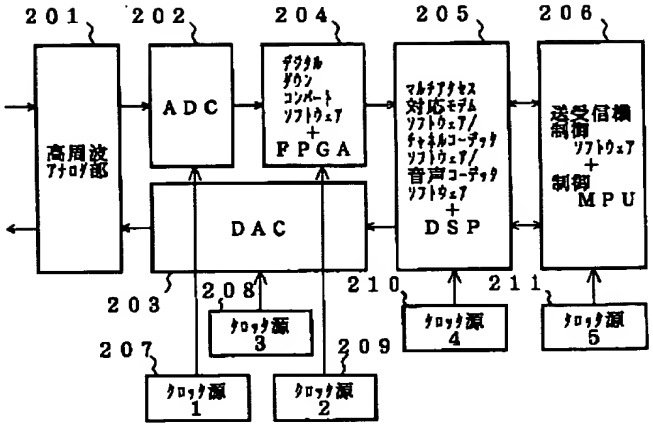
【図１】



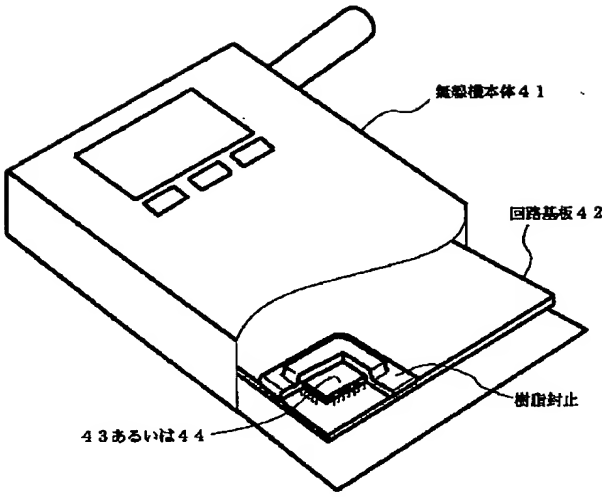
【図２】


電子課金デバイス１２
メモリ１２３
１２５
１２１
公開鍵
MPU
無線機１
１２２
契約している
無線通信
システムの
種類の情報
１２４
着脱情報信号
入出力
I／F
１４
１３
認証
開始
制御部
電子課金デバイス入出力ポート
１５
課金制御部
１６ａ
１０
１１
電源
スイッチ
電源
MPU
２１
２２
メモリ
入出力デバイス
２０
１６
無線通信部
１８
送受信
ソフトウェア
ロード部
１９
ＩＣカードスロット
１７
ＩＣカード

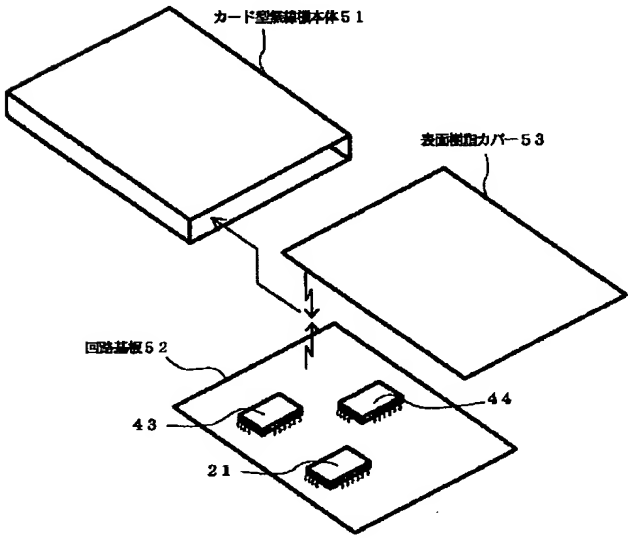
【図３】



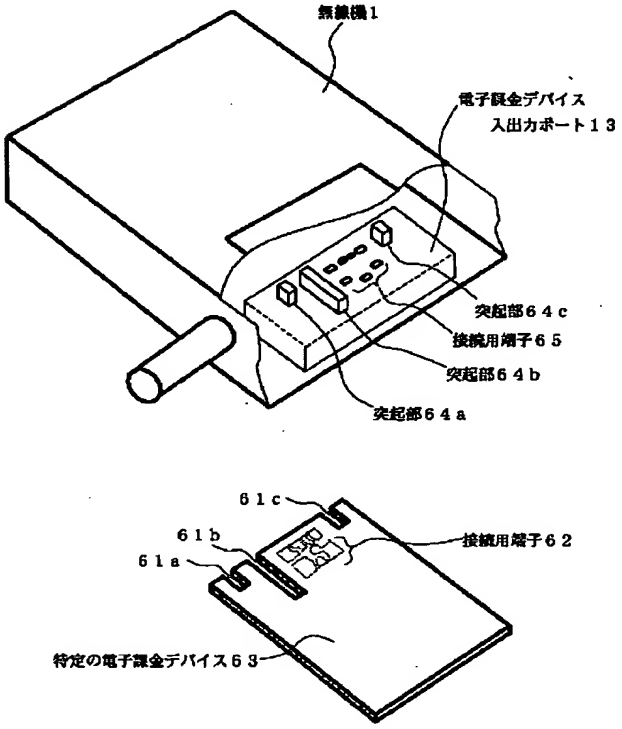
【図４】



【図５】



【図６】



フロントページの続き

(51) Int. Cl.[7]	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ（参考）
		Ｈ０４Ｌ　11/02	Ｆ

Ｆターム(参考)　5J104 AA07 CA01 KA01 MA01 NA41
5K025 AA01 BB02 CC01 DD06 EE18
FF15
5K030 GA15 HB08 HB19 JL01 JT09
KA04 KA23 LD20
5K067 AA29 BB02 DD17 DD27 DD29
EE02 EE10 FF04 GG01 HH22
HH23 HH24 HH36 KK05